CSR Creation and Installation for F5 BIG-IP

How to generate a CSR using an F5 BIG-IP Loadbalancer (version 9)

1. Launch the F5 BIGIP web GUI.
2. Under Local Traffic select "SSL Certificates" then "Create."
3. Under General Properties give your certificate a name (this name will be used in the future to identify this certificate).
4. Under Certificate Properties enter the following information:

   Issuer: Certificate Authority
   Common name: FQDN (fully-qualified domain name) of the server (e.g., www.domain.com, mail.domain.com, or *.domain.com)
   Division: Your department, such as 'Information Technology'
   Organization: The full legal name of your organization
   Locality, State or Province, Country: City, state, and country where your organization is located
   E-mail Address: Your email
   Challenge Password, Confirm Password: Your password
5. Under "Key Properties", choose 2048.
6. Click the Finished button.

   You should now be provided with the text of a Certificate Signing Request file. Please submit the file to us for our process.

CSR Generation (Earlier versions of Big-IP)

1. First, login to the BIG-IP device as the root user and run the following command:

   # /usr/local/bin/genconf
   You will be asked to enter your company details including the full legal company name and address of operation.

2. You can now make your Certificate Signing Request by entering the following command:

   # /usr/local/bin/genkey www.yoursite.com
   Make sure to replace "www.yoursite.com" with the Fully Qualified Domain Name of the site that you are securing.
   You will again be asked to enter your company details.

3. Under /config/bigconfig/ssl.csr/ you will find a new file named your www.yoursite.com.csr -- This is your new CSR file. Transfer it to the workstation you will use to order the certificate. The CSR file can be opened with a text editor such as Notepad. Please send it to us for our process. Make sure to include the BEGIN and END tags.

Install your SSL Certificate to a f5 BIG-IP Loadbalancer (version 9)

Installing the SSL Certificate

4. Launch the F5 BIGIP web GUI.
5. Under Local Traffic select "SSL Certificates."
6. Click on the name you assigned to the certificate under "General Properties" while creating the CSR.
7. Browse to the your_domain_name.crt file that you received.
8. Click "Open" and then "Import."

   Your SSL Certificate file is now installed.

Enabling your Intermediate Certificate

9. In the web GUI, choose "Local Traffic," then "SSL Certificates," and then "Import."
10. Under "Import Type," choose Certificate, then "Create New."
11. Enter "IntermediateCA" as your certificate name.
12. Browse to the IntermediateCA.crt file that you received, click "Open," and then "Import."

Your intermediate certificate should now be imported.

Configure your server for SSL

13. Create or open the SSL Profile that you will be using with this certificate.
14. Log in to the Configuration utility > Local Traffic > Profiles > Client (from the SSL menu), then select the client to configure and choose "Advanced" from the Configuration menu.
15. Select the SSL certificate (public/private key pair) that you installed at the beginning of these instructions.
16. Under the "Chain" section, browse to the "IntermediateCA" file that you imported in the previous step, then save and exit the configuration

    Your SSL Certificate has now been installed and enabled for use on your server.

F5 BIG-IP Pre Version 9.x

Inside your DigiCert account you can download your certificate files. You will need the Primary (your_domain_name.crt) and Intermediate certificate files. You will need both of these files for proper installation on you BIG-IP device. You do not need the TrustedRoot.crt file

17. **Move your Primary and Intermediate Certificates to the BIG-IP device.**
    The Primary (your_domain_name.crt) and Intermediate (intermediate-ca.crt) certificate files can be moved to the BIG-IP box using FTP.

18. **Rename and move the certificate files.**
    Rename your Primary certificate from your_domain_name.crt to your.domain.name.crt and copy it to the /config/bigconfig/ssl.crt/ folder.

    Copy the intermediate-ca.crt to the /config/bigconfig/ssl.crt/ folder.

19. **Restart the Proxy.**
    # bigpipe proxy <*IP Address*>:443 disable
    # bigpipe proxy <*IP Address*>:443 enable
    The Certificate is now installed.